CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

September 29, 2022

Semiconductor Companies Targeted by Ransomware

This report examines ransomware attacks on semiconductor companies to date in 2022. We analyzed the strategic importance of the semiconductor industry and the unique role it plays in the increasingly complex geopolitical environment. We also identified the tactics, techniques, and procedures (TTPs) used by ransomware actors in their attacks.

Executive Summary

We identified 8 semiconductor companies that were attacked and extorted by ransomware actors thus far in 2022. These attacks included the use of LockBit, LV ransomware, and Cuba ransomware, and were conducted by extortion groups including the Lapsus$ Group and RansomHouse. We analyzed the TTPs of each group and the possible motivations behind the attack. In addition, we explored the economic and strategic importance of the semiconductor industry and the crucial role it plays in the geopolitics of US-China/Taiwan, as well as the entire Asia Pacific region. This complex relationship could forebode more cyberattacks against the semiconductor industry by both cybercrime and state-sponsored groups in the near future.

Key Judgments

- Semiconductor manufacturing is a critical industry in today's information technology-driven, globalized economy, which makes it a prime target for ransomware threat actors and extortion groups.
- A variety of TTPs were employed by ransomware threat actors in their attacks against semiconductor companies. Among them are the use of malware to encrypt data; extortion through threat of data exposure; the release of source code and intellectual properties; the use of stolen code-signing certificates to sign malware; and the possibility of selling proprietary data to industry competitors or rival nation-states.
- The motives of ransomware threat actors range from being purely financially driven, to thrill seeking, to the possibly strategic theft of intellectual property.
- While none of the cyberattacks against semiconductor companies analyzed here have direct connections to nation-state groups, industry reports uncovered state-sponsored threat actors masquerading as ransomware groups and using at least 5 ransomware variants — LockFile, AtomSilo, Rook, Night Sky, and Pandora — to conduct cyber espionage.
- In most cases, poor security practices led to initial compromise by ransomware actors, which resulted in the theft of data and information.
- As the competition for semiconductor supremacy is at the heart of the economic competition between China and Taiwan, we believe it is likely that cyberattacks and industrial espionage against semiconductor companies will continue.

Background

According to the Manufacturing Leadership Council, ransomware gangs in 2021 increased their intensity of attacks against all industrial sectors. Manufacturing accounted for 65% of all industrial ransomware incidents in 2021, about 6 times as many as the second leading sector (food and beverage). While semiconductor manufacturing was not listed as 1 of the most affected sub-sectors in 2021, there have been 8 cyberattacks on semiconductor companies so far in 2022, either by ransomware gangs — including LockBit, LV Ransomware, and Cuba Ransomware — or by extortion groups RansomHouse and Lapsus$ Group.

Based on our research, we identified that attacks on semiconductor companies were not necessarily conducted by ransomware operators, but rather by their affiliates using the ransomware-as-a-service (RaaS) and double extortion models. Most top ransomware gangs, including Conti, LockBit, and REvil, have adopted the RaaS business model, where the affiliates use readily available toolkits to execute ransomware attacks and earn a percentage of each successful ransom payment. RaaS enables threat actors without a high level of technical expertise to launch and execute their attacks. In addition, all of the aforementioned ransomware gangs have adopted the double extortion tactic where they leak victim's data on their respective extortion blogs, suggesting that these ransomware groups were not successful in getting a significant number of victims to pay the demanded ransom. This was the case for most of the victims analyzed in this report. We also identified threat actors threatening extortion but not using ransomware when targeting semiconductor firms. This shows that both more technical and non-technical threat actors who have the intention and the will are targeting semiconductor firms.

As semiconductors are the hearts of electronic devices such as smartphones, computers, automobiles, appliances, televisions, and advanced medical diagnostic equipment, any disruption to the semiconductor sector would likely have an impact across all other manufacturing sectors. We believe that ransomware operators see semiconductor companies as high-value targets and leverage media coverage to apply pressure on the victim organization to negotiate and pay the ransom due to the importance of semiconductors to the global economy.

Semiconductor manufacturers have been struggling to keep up with global demand, resulting in a chip shortage that has been ongoing since 2020. We believe that financially motivated ransomware gangs are taking advantage of this opportunity to target semiconductor companies, as any disruption in their operations will have a ripple effect on the global supply chain that is already strained by the COVID-19 pandemic, which increases the likelihood that the affected companies will make the ransom payment. In addition, criminal organizations or nation-state threat actors with the intention of disrupting the global supply chain could do so by targeting the semiconductor industry. We assess that there is a high likelihood that nation-state-backed groups are making use of ransomware belonging to criminal groups to disrupt confidence in the semiconductor manufacturing sector, as well as strategically delaying the ability to expand chip production capabilities. In April 2022, CNBC reported that the continued shortage of semiconductors could "dent GDP growth and boost inflation". The shortage could translate into an inflationary tax that results in prices rising as much as 3% for affected electronics such as cars, televisions, and touch-screen computers, some of which are on backlog orders for 6 months or more.

In 2018, Taiwan Semiconductor Manufacturing Company (TSMC) suffered a major ransomware attack by WannaCry, a group that has alleged ties to North Korea, which led to TSMC shutting down several of its chip fabrication plants. The attack affected more than 10,000 machines in some of TSMC's most advanced facilities, and delayed the production of manufacturing chips that are supposed to be used by Apple's future lines of iPhones, which could affect revenue by approximately $256 million. TSMC also manufactures processors and other silicon chips for global tech giants such as Advanced Micro Devices (AMD), NVIDIA, and Qualcomm.

In 2022, we observed that both AMD — an American multinational semiconductor company based in Santa Clara, California — and NVIDIA suffered a theft of data1 and extortion, respectively; AMD was attacked by the RansomHouse gang in January 2022, and NVIDIA was attacked and extorted by Lapsus$ Group in March 2022. We also observed that semiconductor manufacturers including Samsung, Ignitarium, Diodes Inc., Etron Technology, SilTerra Malaysia Sdn. Bhd., and Semikron have been affected by ransomware attacks so far in 2022.

1 The ransomware group provided access to a free, unsubstantiated sample of data allegedly stolen from AMD.

Table 1: Global Top 10 Foundry Revenue Ranking, 4Q21 (Unit: US$1M)

Ranking	Company	Revenue			Market Share	
		4Q21	3Q21	QoQ	4Q21	3Q21
1	TSMC	15,748	14,884	5.8%	52.1%	53.1%
2	Samsung	5,544	4,810	15.3%	18.3%	17.2%
3	UMC	2,124	2,007	5.8%	7.0%	7.2%
4	GlobalFoundries	1,847	1,700	8.6%	6.1%	6.1%
5	SMIC	1,580	1,415	11.6%	5.2%	5.1%
6	HuaHong Group	864	799	8.1%	2.9%	2.9%
7	PSMC	619	525	17.9%	2.0%	1.9%
8	VIS	458	426	7.4%	1.5%	1.5%
9	Tower	412	387	6.5%	1.4%	1.4%
10	Nexchip	352	244	44.2%	1.2%	0.9%
	Total	29,547	27,277	8.3%	98%	97%

Note 1: 3Q21--1USD:1,160KRW, 1USD:27.9TWD

Note 2: 4Q21--1USD:1,183KRW, 1USD: 27.8NTD

Note 3: Samsung revenue accounts for System LSI and foundry divisions

Note 4: PSMC revenue includes foundry business only

Note 5: Hua Hong Group revenue includes HHGrace and HLMC

Source: TrendForce, Mar. 2022

Figure 1: Top 10 global foundries by revenue as of the fourth quarter of 2021 (Source: TrendForce)

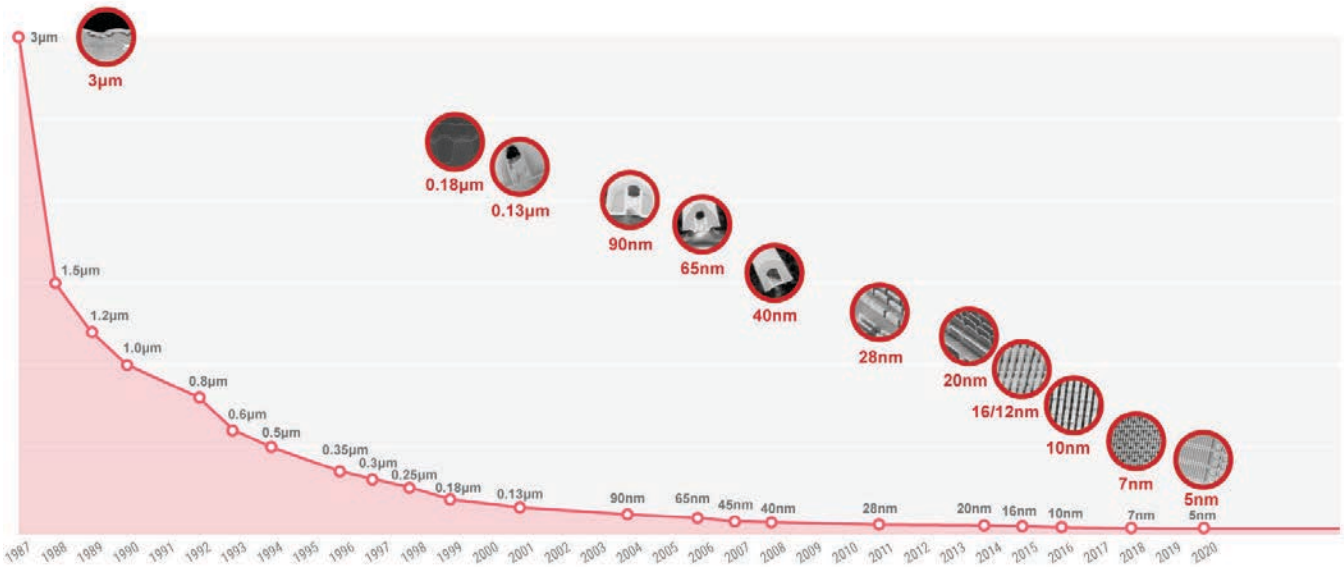

Figure 2: Chronological data of TSMC's semiconductor chip technology growth, with 5nm being the latest and most high-end chip in 2020 (Source: TSMC)

Strategic Importance of Semiconductors to US and China

The US has been adopting a broad and long-standing strategy to deny China access to critical chipmaking technology, and China's Semiconductor Manufacturing International Corp (SMIC) has been sanctioned by the US since September 2020, when the US government cited the potential use of the chipmaker's products in military applications as well as potential ties with the Chinese military.

SMIC planned to produce high-end 7 nm chips during the fourth quarter of 2020 to compete against established semiconductor companies such as TSMC, Intel, and Samsung. SMIC's plan to do so has been negatively affected by US sanctions that prevented SMIC from attaining critically needed equipment and design tools. SMIC has long been considered China's national champion in producing chips and is a company that is expected to lead China's quest for semiconductor self-sufficiency, as semiconductor production is a high-priority issue in China's 2021 five-year plan.

In late July 2022, Tom's Hardware reported that, according to analyst firm TechInsights, SMIC has been producing chips based on its 7 nm process node for a Bitcoin (BTC) Miner SoC, and has been shipping since July 2021. TechInsights reverse-engineered the chip and reported that the initial images are a close copy of TSMC's 7 nm process technology; TSMC sued SMIC twice (in 2002 and 2006) for copying its technology. Asia Times reported that there have been concerns about the failure of American sanctions to stop the advance of Chinese semiconductor technology. Taiwan has also accused China of waging economic warfare against Taiwan's tech sector by stealing technology and poaching engineers, and has concerns that China has been wanting to replicate Taiwan's success in the semiconductor industry by conducting industrial espionage. A migration of the semiconductor industry from Taiwan to China would weaken Taiwan's identity as a major contributor to the global economy, further delegitimizing its claim to governmental autonomy.

According to TrendForce, the top 5 foundries account for nearly 90% of the global market share, with TSMC occupying the top spot with 52.1% and SMIC at the fifth spot with 5.2% as of the fourth quarter of 2021. TSMC has a clear lead in market share amounting to approximately 10 times that of SMIC.

On August 9, 2022, US President Joe Biden signed a bipartisan bill that aims to strengthen US competitiveness with China by investing $52.7 billion in domestic semiconductor manufacturing and science research. The bill, dubbed the CHIPS (Creating Helpful Incentives to Produce Semiconductors) and Science Act of 2022, includes both investment and tax credits to encourage investment in semiconductor manufacturing. The bill includes $39 billion in manufacturing incentives, including $2 billion for the legacy chips used in automobiles and defense systems, $13.2 billion in R&D and workforce development, and $500 million to provide for international information communications technology security and semiconductor supply-chain activities. It also provides a 25% investment tax credit for capital expenses for manufacturing of semiconductors and related equipment. These incentives are aimed at securing domestic supply, creating tens of thousands of lucrative union construction jobs and thousands more high-skilled manufacturing jobs, and catalyzing hundreds of billions more dollars in private investment. A similar act was proposed in the European Union in February 2022.

To take advantage of the funds, "Subsidy recipients are barred from expanding production in China beyond 'legacy semiconductors' — defined as chips made with 28-nanometre process technology or older— for 10 years." The law is designed to attract semiconductor talent and investments to the US, while trying to stop global chip giants such as TSMC and Samsung Electronics from expanding their capacity in China using US funding. China's foreign ministry has strongly opposed the bill because it includes clauses restricting investments in the country.

China is still behind the US, Taiwan, and South Korea in terms of semiconductor chip manufacturing capabilities. The US initiated the Chip 4 alliance consisting of the US, Taiwan, South Korea, and Japan, with the strategic objective of excluding China from semiconductor value chains; this initiative has been condemned and opposed by China. The Chinese government claims that the US is trying to "weaponize" the chip supply issue, and has urged South Korea not to join the chip alliance.

China is dedicated to obtaining new manufacturing technologies to compete with the US, and has targeted the chip industry by stealing intellectual property. We assess that in addition to nation-state threat actor groups, financially motivated ransomware groups have a stronger incentive to attack, steal, and encrypt data. Ransomware attacks can steal information that could prove potentially advantageous to the growth and advancement of the Chinese semiconductor industry, as well as achieving the strategic goal of delaying the production processes and advancement of the US semiconductor industry and its allies, particularly Taiwan, South Korea, and Japan.

Notable Intellectual Property Theft and High-Risk Incidents

Case Study 1: SMIC Recruited Many Engineers from TSMC

South China Morning Post reported that many of SMIC's engineers, including key senior managers, were recruited from Taiwan, notably from TSMC, and that SMIC has been sued by TSMC for alleged intellectual property theft in hiring former TSMC employees. Reuters also reported in May 2022 that Taiwan raided 10 Chinese companies suspected of illegally poaching chip engineers and tech talent, in a bid to protect its semiconductor chip industry's secrets and to prevent China from obtaining crucial chip-making technology.

Case Study 2: Chinese National Sentenced to Jail for Stealing Trade Secrets

In September 2020, ZDNet reported that a Chinese national, Hao Zhang, had been sentenced to 18 months in US prison by the District Court of Northern California for stealing trade secrets from semiconductor companies Avago Technologies and Skyworks Solutions Inc. Zhang stole trade secrets such as semiconductor recipes, source code, specifications, presentations, design layouts, and other confidential information from these companies. The trade secrets were reportedly shared with Tianjin University to enable the construction of a semiconductor fabrication plant and a China-based semiconductor business.

Case Study 3: Japanese Police Put Out High Alert for Potential Espionage Attempt by Russian Individual

On July 28, 2022, Japan's police authorities alerted multiple Japanese semiconductor companies that a staff member of Russia's Trade Representation had been in contact with employees belonging to Japanese semiconductor firms. The Japanese police believe that the staff member may have been engaged in espionage activities, and was attempting to steal the companies' technological information. The alerting of semiconductor firms is part of the Japanese government's economic security measures to prevent technology transfer to other nations.

Rising US-China Tensions and Speaker Pelosi's Visit to TSMC

On August 2, 2022, US House of Representatives Speaker Nancy Pelosi traveled to Taiwan amid threats of Chinese retaliation, demonstrating a significant show of support for Taiwan. China's Ministry of Foreign Affairs (MoFA) strongly condemned the visit2, calling it a "serious violation of the One-China policy and provisions of the 3 China-US joint communiques". The Chinese government summoned the US Ambassador to China, Nicholas Burns, to protest the visit. China also warned of serious consequences for both Taiwan and the US. On August 3, 2022, China's military launched large-scale air and sea exercises surrounding Taiwan. Additionally, China restricted trade with Taiwan, halted exports of sand for semiconductor production, and restricted imports of Taiwanese citrus fruit and certain types of fish.

As part of Speaker Pelosi's visit to Taiwan, she met with TSMC chairman Mark Liu on August 3, 2022, where they discussed the aforementioned CHIPS and Science Act, a law that is perceived as Washington's plan to strengthen the US's role in global semiconductor supply chains. At the same time, the meeting also demonstrated the strategic importance of Taiwan and TSMC, which supplies high-end semiconductors that are vital to both the US and China's technological advancement. Prior to Speaker Pelosi's visit, TSMC Chairman Liu remarked that if China were to invade Taiwan, the most advanced chip factory in the world would be rendered "not operable", and warned that a Taiwan-China military conflict would have serious economic consequences for China, Taiwan, the US, and Western countries in general.

Russia, a close ally of China, condemned Speaker Pelosi's visit to Taiwan. Maria Zakharova, Russia's foreign ministry spokeswoman, said the visit was a provocative attempt by Washington to put pressure on China, with whom Russia has forged a strong partnership in recent years. "The USA is a state provocateur", she said. "Russia confirms the principle of 'one China' and opposes the independence of the island [of Taiwan] in any form".

2 https://www.fmprc[.]gov[.]cn/eng/zxxx_662805/202208/t20220802_10732293.html

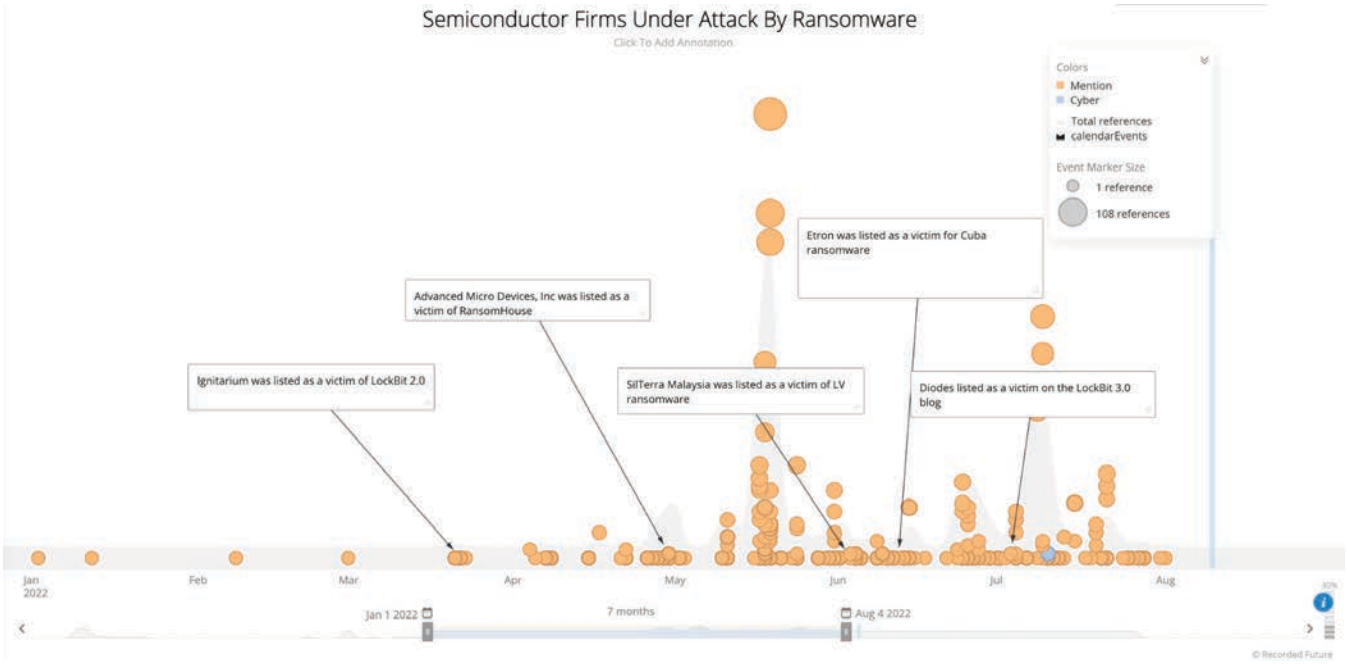

Figure 3: Major ransomware attacks against semiconductor companies in the first half of 2022 (Source: Recorded Future)

Threat Analysis

Through research across dark web ransomware extortion blogs and Telegram channels of ransomware and extortion threat actors, we have identified the following semiconductor companies that were attacked and also analyzed the TTPs of these ransomware and extortion groups.

Lapsus$ Group — NVIDIA (USA) and Samsung (South Korea)

NVIDIA

We do not consider Lapsus$ Group to be a ransomware gang, but rather a low-level threat group that is financially motivated and specializes in data extortion. The TTPs exhibited by the group are different when compared to other ransomware groups. The Lapsus$ Group does not deploy ransomware, but rather exfiltrates data via the following attack vectors:

- Phishing and website defacement
- Large-scale social engineering and extortion campaigns against multiple organizations with the use of the following:
    - Deploying RedLine infostealer to obtain passwords and session tokens
    - Purchasing credentials and sessions tokens from criminal underground forums and shops
    - SIM Swapping
    - Exploiting unpatched vulnerabilities on internally accessible servers, including JIRA, GitLab, and Confluence
    - Searching code repositories and collaboration platforms for exposed credentials and proprietary information

On February 25, 2022, Lapsus$ Group, also known as "DEV-0537", announced that it had exfiltrated 1 TB worth of data from US chipmaker NVIDIA. As with typical double extortion campaigns from ransomware groups in the past few years, Lapsus$ Group threatened to publish the data if NVIDIA failed to pay the ransom demand. 1 of Lapsus$ Group's more specific avenues for extortion was to threaten the release of information about how to bypass Lite Hash Rate (LHR) limiters in certain NVIDIA chipsets (GA102 and GA104). LHR refers to a NVIDIA technology that limits the rate of hashing when the chip detects that it is being used to mine for Ethereum (ETH). Additionally, the attack reportedly caused NVIDIA's internal systems such as email to go offline for 2 days, and Lapsus$ Group claimed in their initial post that they exposed a text file containing hashed passwords of all NVIDIA employees. Multiple messages from the threat group indicated that they had access to NVIDIA networks for about 1 week, stealing data related to schematics, drivers, and firmware, including Falcon, a special class of microcontroller inside all of NVIDIA's graphic processing units (GPUs).

Lapsus$ Group's threat to release information about LHR-limiting is very likely based on their understanding of the GPU market, which in the last few years has suffered supply shortages and high prices due to cryptocurrency miners' reliance on GPUs, as cryptocurrency miners competed with gamers worldwide to purchase all available GPUs for both mining and gaming purchases. GPUs are essential for PC gamers to play the latest-generation video games at higher resolutions and response times, as GPUs ensure a smooth visual experience for gamers. Pricing for GPUs has only started to drop due to the wider decrease in cryptocurrency prices (specifically for Bitcoin and Ethereum) over the past several months. LHR-limiting separately raised security concerns in the past few weeks due to reports that a tool that was advertised as being able to bypass the technology was found to deploy a trojan. Together, these episodes highlight the ongoing interest in the cryptocurrency ecosystem by cybercriminals.

As pointed out by Tech Radar, Lapsus$ Group's threat to release LHR-limiting specifications contradicts their request that NVIDIA undo this limitation on their own in exchange for data not to be leaked. This contradiction indicates a strong likelihood that either Lapsus$ Group does not understand how a bypass would work, or they do not have this data and are attempting to bluff that they do in order to assist their own or others' cryptocurrency mining efforts.

After Lapsus$ Group leaked NVIDIA's code-signing certificates in February 2022, security researchers found that the leaked certificates were being used to sign malware, enabling malicious programs to pose as legitimate and slide past security safeguards on Windows machines.

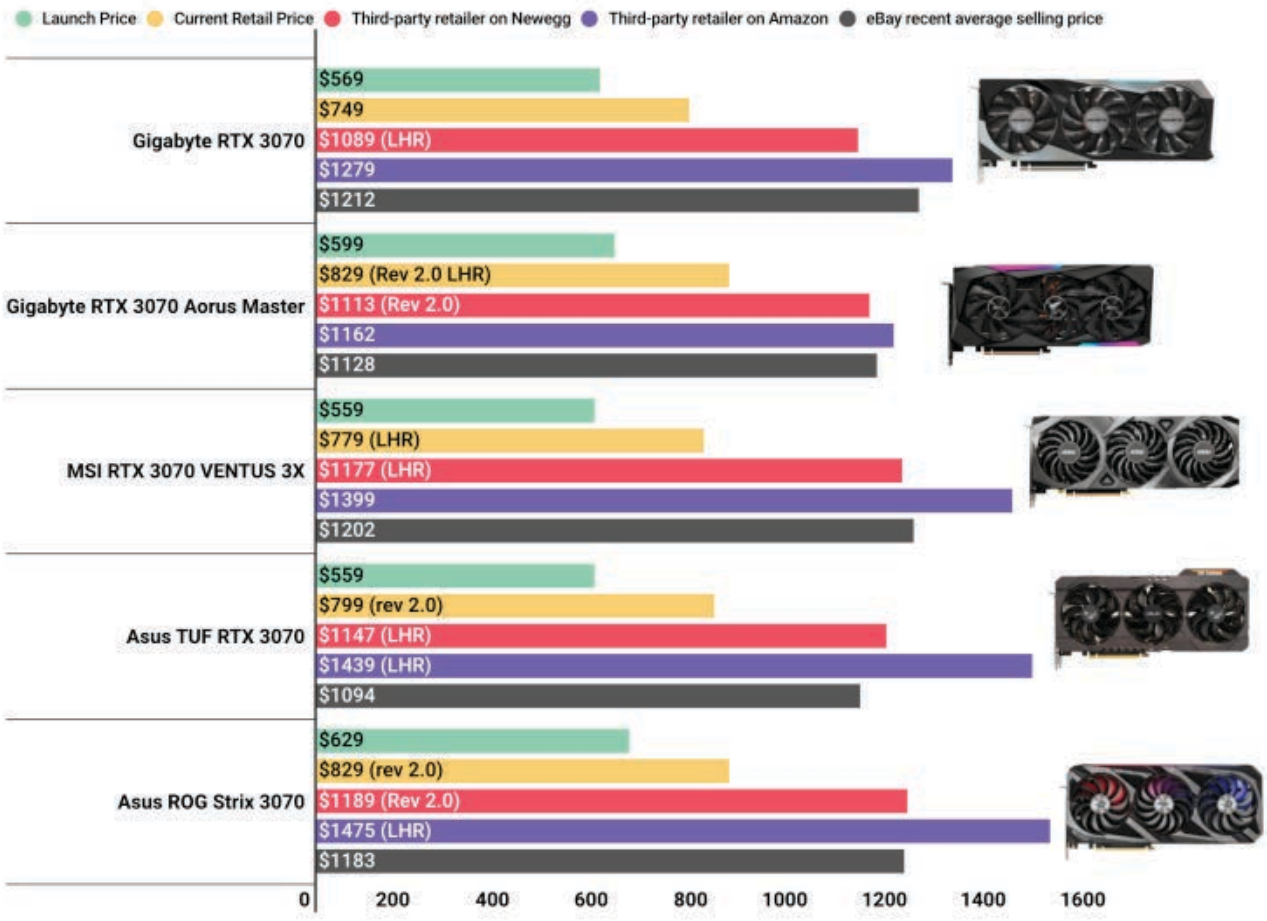

Figure 4: Nvidia's RTX 3070 GPU pricing was much higher in November 2021 than at the time of its launch in 2020 (Source: PCMag)

The attack in February 2022 resulted in 20 GB of data being harvested from the GPU maker, a haul that included data on hardware schematics, firmware, drivers, email accounts, and password hashes for more than 71,000 employees. The group began leaking this data online after NVIDIA refused to negotiate with them. The leak included 2 stolen code-signing certificates used by NVIDIA developers to sign their drivers and executables. While both stolen NVIDIA certificates are expired, Windows will still allow a driver signed with the certificates to be loaded in the operating system. According to the security researchers, malicious binaries were being signed with the stolen certificates to spoof legitimate NVIDIA programs, which appeared in the malware sample database VirusTotal.

According to reports, the signed binaries were detected as Mimikatz, a tool for lateral movement that allows attackers to enumerate and view the credentials stored on the system; malware and hacking tools were also detected, including Cobalt Strike beacons and backdoors and remote access trojans (RATs) that include QuasarRAT.

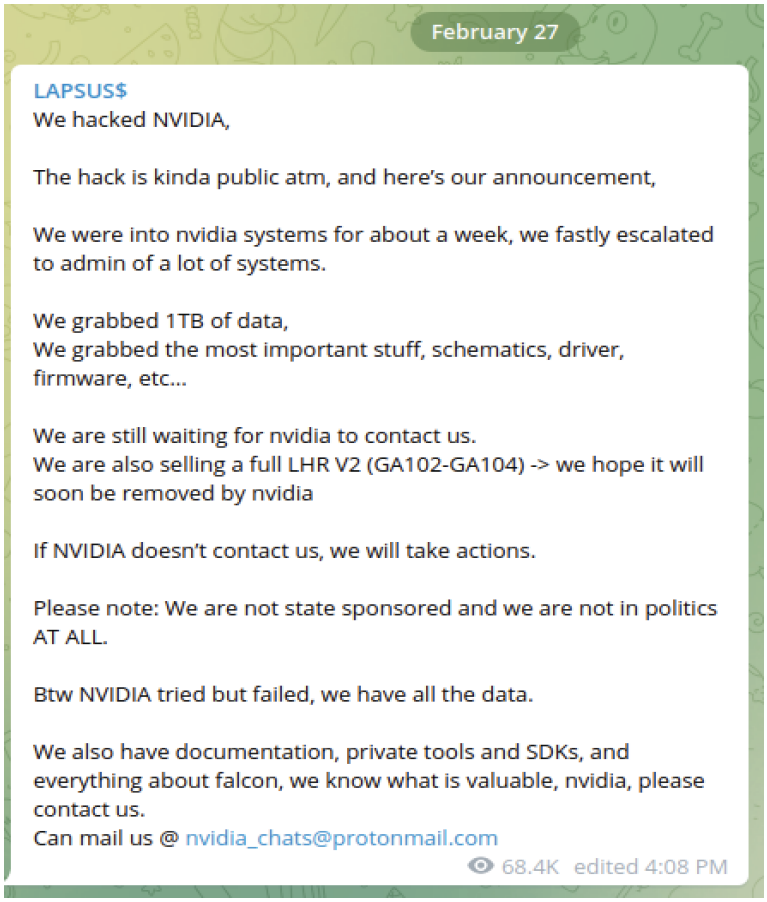

Figure 5: In February 2022, Lapsus$ Group claimed to have exfiltrated 1 TB of data from NVIDIA (Source: Telegram)

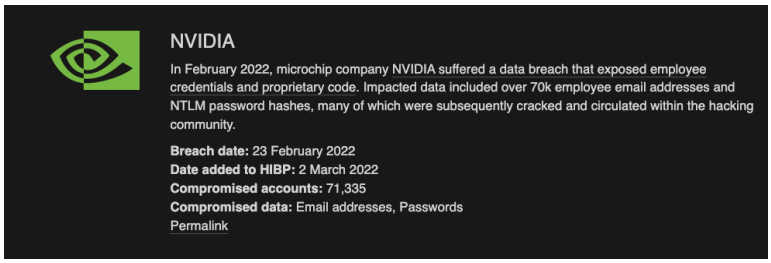

Figure 6: Details regarding NVIDIA's data breach that included 71,335 employee email addresses and NTLM password hashes (Source: haveibeenpwned)

Samsung

The Lapsus$ Group claimed responsibility for leaking stolen data from Samsung Electronics, according to a Security Affairs report on March 5, 2022. The stolen data purportedly included:

- Source code for every Trusted Applet (TA) installed in Samsung's TrustZone environment used for sensitive operations
- Algorithms for all biometric unlock operations, including source code that communicates directly with the sensor
- Bootloader source code for all recent Samsung devices, including Knox data and code for authentication
- Various other data, including confidential data from Qualcomm
- Full source code for technology used for authorizing and authenticating Samsung accounts, including APIs and services

Lapsus$ Group split the leaked data into 3 compressed files. The availability of the sample data was announced on its Telegram channel and shared with a torrent file to download it. The torrent file also provides a summary for the content available in 3 compressed files:

- Part 1 contained a dump of source code and related data about Security/Defense/Knox/Bootloader/TrustedApps and various other items
- Part 2 contained a dump of source code and related data about device security and encryption
- Part 3 contained various repositories from Samsung GitHub: mobile defense engineering, Samsung account backend, Samsung pass backend/frontend, and SES (Bixby, Smartthings, store)

On March 7, 2022, Samsung confirmed to Bloomberg that certain internal company data was exposed to an unauthorized party following a security breach. Based on Samsung's initial investigation, the breach is limited to source code relating to the operation of Galaxy devices, but did not include the personally identifiable information (PII) of customers and employees.

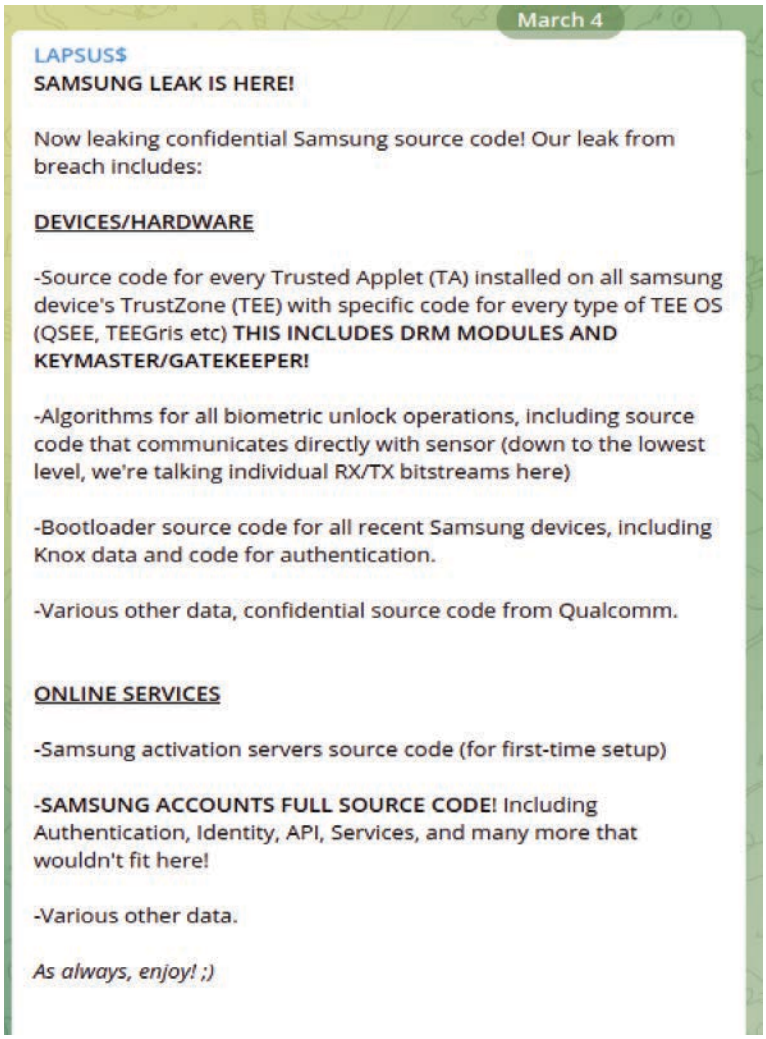

Figure 7: In March 2022, Lapsus$ Group threatened to leak Samsung source code on its Telegram channel (Source: Telegram)

Arrests

On April 1, 2022, the City of London Police disclosed that 2 unnamed teenagers, a 16-year-old and a 17-year-old who were allegedly linked to Lapsus$ Group, had been charged with engaging in malicious activities.

According to Michael O'Sullivan, detective inspector from the City of London Police, 3 counts of unauthorized access on a computer with intent to impair the reliability of data was observed in the investigation, as well as 1 count each of fraud by false representation and unauthorized access to a computer to disable access to victim's data. In addition, the unnamed 16-year-old was charged with a count of enabling a computer to perform a secure unauthorized access to a program function.

Both individuals charged in the investigation are considered juveniles, which restricts the disclosure of their identification. The 2 unnamed teenagers are included in the 7 suspects in the campaign that leaked 70 GB of data belonging to software services giant Globant on March 30, 2022, an incident that is still under investigation.

LockBit 2.0 — Ignitarium (India) and LockBit 3.0 — Diodes (USA)

According to the ransomware victimology compiled by The Record by Recorded Future, LockBit ransomware, which began operating in 2019, overtook Conti to become the most prolific ransomware in terms of publicly claimed victims. Based on research by Mandiant, multiple LockBit ransomware intrusions were attributed to UNC2165, a financially motivated threat actor group that shares numerous overlaps with the group publicly reported as Evil Corp.

The LockBit Gang, the operators of LockBit ransomware, claimed 2 semiconductor companies as victims during the past 5 months. The first was Ignitarium (ignitarium[.]com), a boutique silicon and embedded system design house in India, which first appeared on March 23, 2022 on LockBit 2.0 Leaked Data (LockBit 2.0's extortion blog). The second was Diodes, Inc. (diodes[.]com), a global semiconductor manufacturer headquartered in Plano, Texas, US, whose stolen data was first uploaded onto the revamped LockBit 3.0 blog named LockBit 3.0 Leaked Data on June 29, 2022. In the Ignitarium case, the stolen data, which included the company's source code, was free to download. In the Diodes case, the threat actor claimed to have 2 TB of company data, including technical documents such as "datasheets, X-ray photos, instructions, tests, engineer comments, production costs, and wafer fabrication schemes". The data package also allegedly included company "confidential information" such as "bank documents, contracts with the computer equipment manufacturers, order and shipment paperwork, [and] internal company correspondence, including bank correspondences and correspondences with client companies". The ransom note also included specific instructions, such as:

- A payment of $10,000 is required to extend the deadline for data release by 24 hours
- A payment of $14,453,391 to destroy all the information
- In addition, one can pay $14,453,391 to download the data at any moment

The threat actors also set up the following wallets for payments:

- BTC wallet: bc1q9elveqafa7m2e0vdeenjp46qukvjjgpffh2rys
- Monero (XMR) wallet: 48XyFEbDz4117SopGgaSjAaMK2uXqvnmq7W2wFXKUFPJNdTLFUvgKyx82jcRiWXBDv9ojbijGYyqz9edtrsgZG9NMHG7Xff

No payment/transaction has appeared in those wallets at the time of this report.

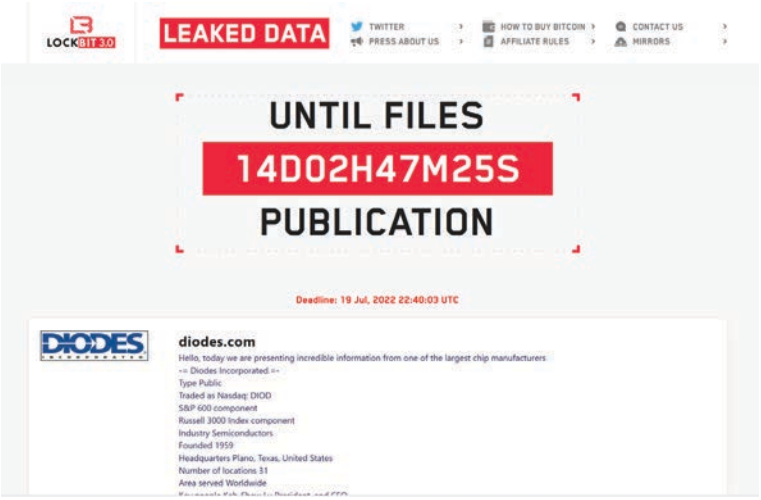

Figure 8: Announcement of the Diodes Inc. hack with a countdown timer for data release on the extortion website of LockBit 3.0 (Source: LockBit 3.0 Leaked Data)

LockBit 2.0

In June 2021, an updated version of LockBit ransomware called LockBit 2.0 ransomware emerged, which followed the RaaS model allowing "affiliates to utilize it as desired, provided a percentage of the illicitly gained profits are shared with the LockBit operators as commission", according to the Australian Cyber Security Centre (ACSC). LockBit 2.0 has been responsible for attacks on a global scale. In addition, since LockBit 2.0 first started posting to their extortion website, LockBit 2.0 Leaked Data, on July 13, 2021, we have identified references to organizations in the following sectors: software, automotive, banking, hospitality, information technology, retail, services, telecommunications, and more. LockBit 2.0 has been observed exploiting an existing vulnerability in the Fortinet FortiOS and FortiProxy products, tracked as CVE-2018-13379, in order to gain initial access to specific victim networks.

LockBit 3.0

On June 27, 2022, the LockBit Gang launched its newest RaaS operation, LockBit 3.0. LockBit Gang also inaugurated a bug bounty program, reportedly the first of its kind available on the dark web, in which the RaaS group is soliciting bug report submissions from security researchers in exchange for payouts anywhere from $1,000 to $1 million.

It is unclear at this time what technical changes LockBit Gang has made to its encryptor; however, the ransom notes are no longer named "Restore-My-Files.txt", and instead have moved to the format [id]. README.txt. According to BleepingComputer, with the launch of LockBit 3.0, the threat group has also adopted a new extortion model in which it gives interested buyers the chance to buy stolen data while LockBit 3.0 attacks are still underway. Depending on the volume of stolen data, buyers can either download it directly or through Torrents for larger packages. In addition, researchers at Trend Micro pointed out that portions of LockBit 3.0's code seem to be borrowed from BlackMatter ransomware, hence the nickname LockBit Black.

The bounty program is a revamped RaaS program that offers rewards for PII on high-value targets, as well as web security exploits. LockBit Gang is offering bounties for other categories as well, including: website bugs, encryption bugs, doxxing, TOX messenger, and TOR network. In the same posts on its bug bounty page, LockBit Gang also solicited innovative methods and ideas for how it can improve its ransomware operation. According to its extortion website, LockBit Gang is accepting ransom payments in its usual cryptocurrencies, BTC and Monero (XMR), but it has announced that it will now also accept Zcash (ZEC).

RansomHouse — AMD (USA)

On May 1, 2022, we identified that AMD was listed on RansomHouse's website. The threat actors claimed to have exfiltrated 450 GB worth of data from AMD, including research and financial information. The threat actors provided a free sample of the data for download that contained more than 77,000 allegedly compromised devices belonging to AMD, and mocked the alleged victim for having poor security by using easy-to-guess passwords.

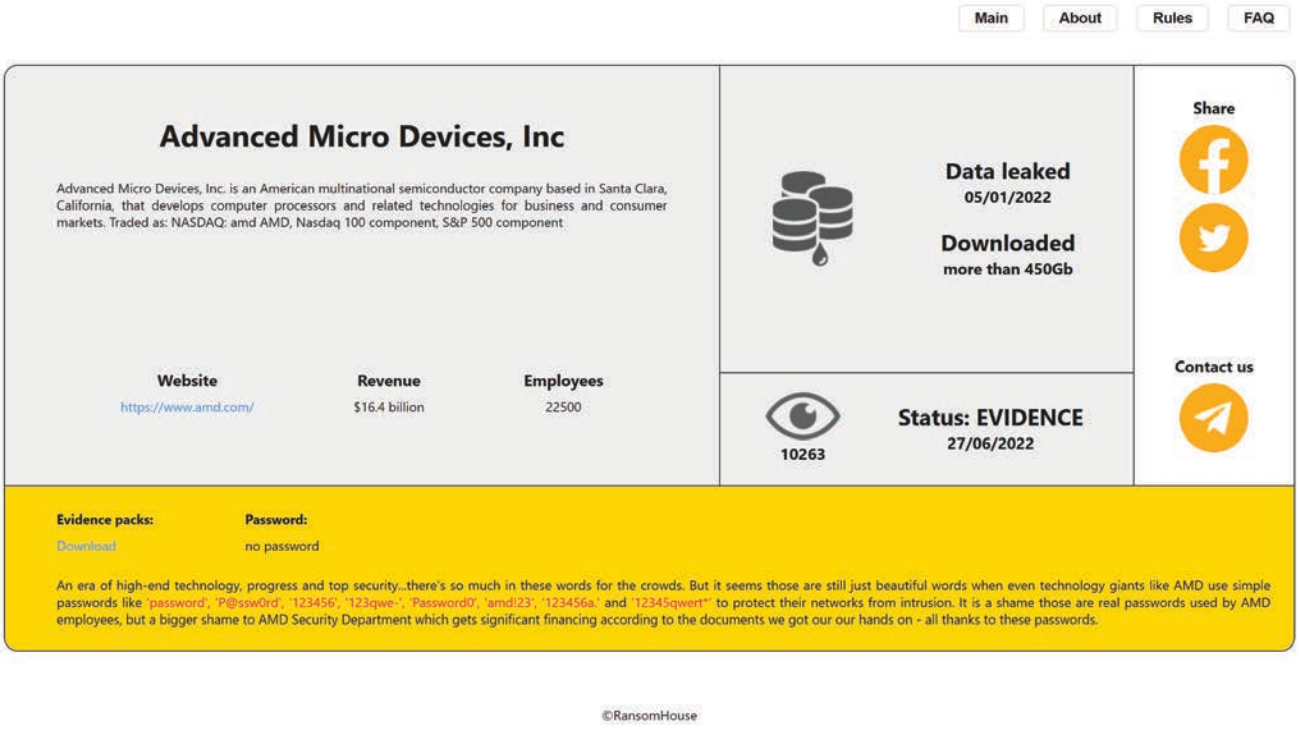

Figure 9: RansomHouse posted data belonging to AMD on its extortion website and mocked its poor security (Source: RansomHouse)

RansomHouse claims not to use any ransomware and instead focuses on breaching networks through unpatched vulnerabilities to steal victims' data. It emerged in December 2021 after attacking its first victim, the Saskatchewan Liquor and Gaming Authority (SLGA). It also lists NVIDIA and Samsung, who were also compromised by Lapsus$ Group, as its victims.

According to Emisoft's threat analyst Brett Callow, the RansomHouse platform is supposedly used by "club members" who carry out attacks using their own tools, including the White Rabbit ransomware. However, this differs from other claims that RansomHouse does not encrypt victim data using a ransomware strain, and that their extortion is based solely on the threat that RansomHouse makes to expose stolen files. Cyberint's May 23, 2022 report noted that the more widely known data theft and extortion group Lapsus$ Group promoted RansomHouse on its Telegram channel. While RansomHouse's exact origin remains unclear, Cyberint researchers believe that the threat group consists of experienced red-team pentesters based on some of their communications on Telegram, which Cyberint monitored.

LV Ransomware — SilTerra Malaysia Sdn. Bhd. and Semikron

On June 4, 2022, we identified that SilTerra Malaysia Sdn. Bhd., a Malaysia semiconductor manufacturer, was listed on the LV Blog ransomware extortion website operated by LV ransomware. The company, which was formerly known as Wafer Technology, was founded in 1995. According to the threat actors, the 1 TB worth of compromised data includes business planning documents, insurance information, financial data, employee data, client data, and more, all of which were available to download.

On August 4, 2022, we also identified Semikron, a Germany-based independent manufacturer of power semiconductor components, as being listed as a victim on the LV blog extortion website. The threat actors claimed to have stolen 2 TB worth of data from Semikron including NDAs, drawings, employee data, contracts, financial data, investment data, and customer data. In addition, the threat actors claimed that Semikron networks have many backdoors and vulnerabilities, and directed visitors to the extortion blog to another TOR-based website to access 10% of the available data. A qTox handle was also included for negotiation for data acquisition.

While we could not identify the attack vectors that led to the ransomware attacks against SilTerra Malaysia and Semikron, we believe that LV ransomware, also known as ".0nzo8yk Virus" and identified in the wild as early as June 2020, is a modified version of the ransomware variant REvil/Sodinokibi v2.03 adopted by the operators of the LV Ransomware Gang. Among the primary technical updates of the malware implemented by LV Ransomware Gang was the removal of command-and-control (C2) servers, which were used by the REvil operators to track infections and replaced with their own servers. We have not identified any advertisements, sales, or hiring of affiliate partners of LV ransomware on dark web forums or other sources.

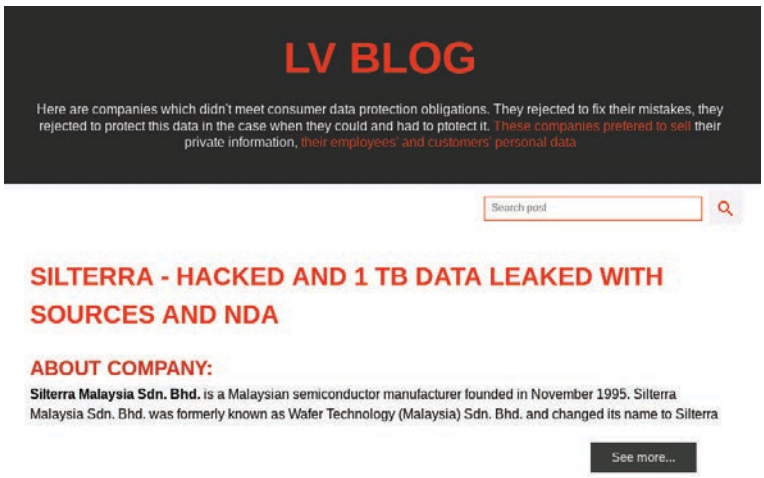

Figure 10: LV ransomware extortion blog claims that the group stole 1 TB worth of data from SilTerra Malaysia Sdn. Bhd. (Source: LV Blog)

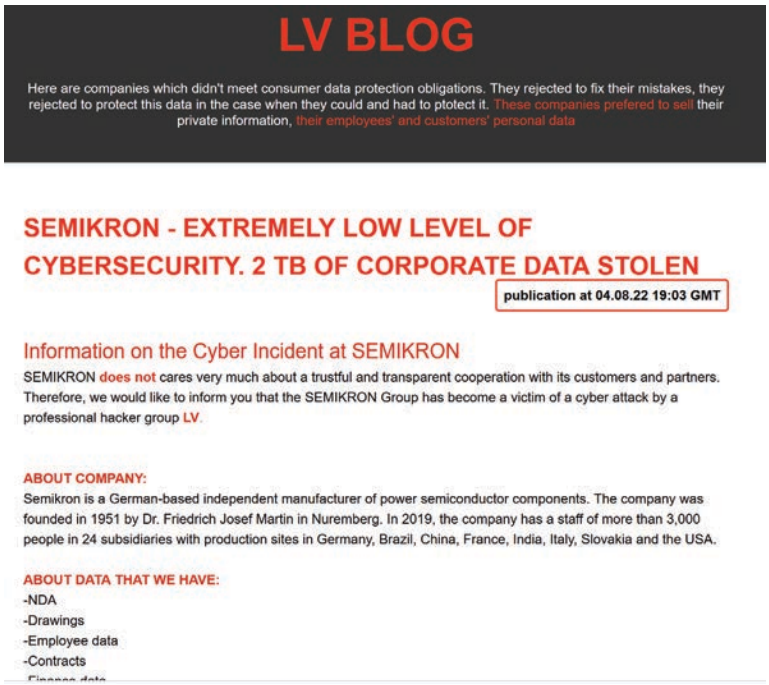

Figure 11: LV ransomware extortion blog claims that the group stole 2 TB worth of data from Semikron (Source: LV Blog)

Cuba Ransomware — Etron Technology (Taiwan)

On June 13, 2022, a post from Cuba Leaks, the extortion website of Cuba Ransomware, claimed that they first received files from Etron Technology (etron[.]com), a fabless IC design and production company, on June 1, 2022. The financial documents, correspondence with bank employees, account movements, balance sheets, tax documents, compensation, and source code are all available to download. On June 8, 2022, Trend Micro Inc. reported on a new variant of Cuba Ransomware Gang's ransomware being used in 2 attacks targeting Asia-based organizations in late April 2022.

Etron Technology was founded in February 1991 and specializes in buffer memory and system-on-chips. Etron Technology pioneered3 Taiwan's "National Sub-micron Project" and helped develop Taiwan's first 8-inch wafer sub-micron technology, building a solid foundation for the DRAM and SRAM industries in Taiwan. As a publicly traded company headquartered in Taiwan, Etron Technology strives to bridge the borders between the Asia Pacific region and the international marketplace. It conducts active business with companies in the US, Europe, Japan, as well as in other Asian countries.

Since Cuba Ransomware Gang first emerged in February 2020, its malware has resurfaced many times with new variants. The latest variant, spotted in late April 2022, displayed optimized execution and infection techniques. The update enabled Cuba Ransomware to better terminate processes and services including in Microsoft Outlook, Microsoft Exchange, and MySQL. These services and processes are terminated so that more files and applications in the infected system can be encrypted. The full list of the processes and services affected by the ransomware is made available on Trend Micro's report.

Another noted difference in the April 2022 variant is its expanded safelisted directories and file types. This newest variant of Cuba Ransomware will therefore avoid more directories and file types during encryption. This is likely done in order to avoid detection. In addition, Cuba Ransomware Gang retained only 2 commands in the new variant that are directory- or location-related phrases. Former variants, like the 1 seen in March 2022, contained more commands and functions. The adversaries also updated their ransom note to state that the exfiltrated data will be published on their extortion website if the victims refuse to negotiate with the adversaries in an allotted amount of time. This signifies a new intention to use the double extortion method of launching DDoS attacks against victims. The ransom note also features "qTox", which facilitates live technical support for the victim's ransom payment negotiations.

3 https://etron.com/aboutus/company/

The timing of the attack and the announcement of Etron Technology as a victim indicate that the new variant was most likely used in the attack of Etron Technology. It also indicates that Etron Technology most likely refused to pay the ransom during the allotted time for negotiation, which resulted in their data being disclosed on Cuba Leaks.

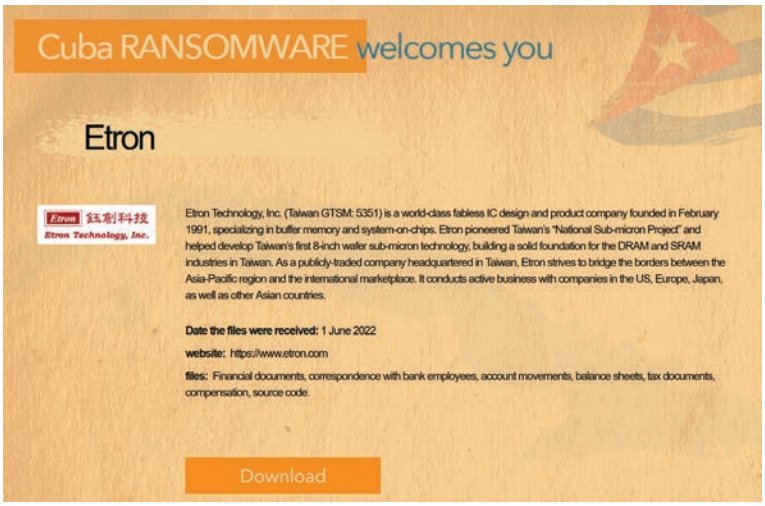

Figure 12: Cuba Ransomware posted data belonging to Etron Technology on its extortion website (Source: Cuba Leaks)

Ransomware Affiliate Rules on Not Encrypting Data Belonging to Critical Infrastructure

Ransomware affiliates are only known to ransomware operators and have to follow certain rules set by the ransomware operators. For example, LockBit 3.0 operators allow affiliates to work with other ransomware operators, but want the affiliates to report such activity and explain why they did it and what they like in their competitors. LockBit 3.0 also explicitly bans affiliates from encrypting files in critical infrastructure such as nuclear and thermal power plants, which we believe is a measure to prevent the US State Department from diverting resources to clamp down on the ransomware operator. However, semiconductor companies are not clearly defined as critical infrastructure on their affiliate rules page, which could technically allow affiliates to not just steal data, but also encrypt files belonging to semiconductor firms. Such affiliate programs can be seen as a win-win scenario for both threat groups and ransomware operators, as threat groups can make use of existing ransomware families to encrypt and steal information belonging to semiconductor firms, and ransomware operators, who are primarily financially motivated, get a cut of the ransom being demanded by the threat group.

Rules of the affiliate program:

You must be active to work with our software package.
It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.
It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.
It is imperative to download valuable information from every company you attack. If you can't bypass your firewall settings and you don't have the ability to download the information, then perhaps our proprietary StealBit Stealer can help you.
It is not forbidden to work with competitors, but be sure to report it and explain why and what you like from your competitors, we will implement any of your worthy wishes, we care very much about progress and constant development.

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.
The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.
It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

Figure 13: LockBit 3.0's rules allowing affiliates to work with other ransomware operators, and explicitly banning affiliates from encrypting files belonging to companies in critical infrastructure. However, affiliates are allowed to steal data belonging to critical infrastructure without encryption. (Source: LockBit 3.0 Leaked Data)

Any cyber threat group that crosses the line and targets US-based critical infrastructure will likely be subject to indictment by the US government. On August 11, 2022, the US State Department announced a reward of up to $10 million for anyone who can provide information on 5 high-ranking Conti ransomware members — the Rewards of Justice Program provides monetary rewards for information related to threat actors affecting the national security of the US. BleepingComputer reported that although the Conti ransomware brand has shut down, the members are still fully active and operating in other ransomware operations and extortion groups. Because the Rewards of Justice Program also incentivizes individuals to provide information about foreign-linked malicious cyber activity targeting US critical infrastructure, it is unlikely that foreign threat groups would want to risk being identified and having bounties placed on them. We believe that it is easier for these threat groups to conduct cyberattacks by using existing ransomware families to prevent direct attribution to these groups.

Figure 14: US State Department offering a monetary reward of up to $10 million for information about any individual that partakes in malicious cyber activity targeting US critical infrastructure, including those acting at the direction or under the control of a foreign government (Source: US State Department)

The US Cybersecurity and Infrastructure Security Agency (CISA) lists 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the US that their incapacitation or destruction would have a debilitating effect on national security, national economic security, national public health or safety, or any combination thereof. The semiconductor industry is not currently defined by the US government as being a critical infrastructure sector, and it is also not explicitly listed under the critical manufacturing sector. But while the semiconductor industry may not be listed as a critical infrastructure sector as of this writing, with the growing recognition of its strategic importance, as well as the US government's plan to support domestic chip production, we believe that there is a strong likelihood that the US government may classify semiconductor firms as a critical infrastructure sector in the future, which will serve as a new deterrent to prevent ransomware affiliates from targeting this industry.

We also believe that nation-state threat actors may have already become affiliates with RaaS operators and are using different ransomware families to conduct cyberattacks with the main objective of stealing IP from semiconductor companies. By doing so, these nation-state threat actors can make use of readily available ransomware to encrypt and steal information, and make the cyberattacks look like attacks from ransomware groups. As attacks on high-profile targets such as critical infrastructure and semiconductor firms draw public attention around the world, threat groups often operate under the guise of anonymity, diverting attribution to ransomware groups instead.

Chinese APT Group Using Ransomware Attacks as Cover for IP Theft

While we did not find direct links between state-sponsored threat activity groups and the cyberattacks on semiconductor companies described in this report, researchers at Secureworks did uncover Bronze Starlight, a China-based APT actor that has been active since 2021. Bronze Starlight is using ransomware and double-extortion attacks as camouflage for systematic, state-sponsored cyber espionage and intellectual property theft. Secureworks reported that three-quarters of Bronze Starlight's victims are organizations that have typically been of interest to state-sponsored Chinese cyber-espionage groups, which includes pharmaceutical companies, electronic component designers, and manufacturing firms. The APT group has used at least 5 ransomware variants in its attacks, namely: LockFile, AtomSilo, Rook, Night Sky, and Pandora. The group uses a double-extortion tactic by encrypting sensitive data and threatening the victim organizations that it will leak their data publicly, allowing Bronze Starlight to appear to be financially motivated on the surface.

However, Secureworks claims that the real objective appears to be cyber espionage and intellectual property theft to support Chinese economic objectives, and that the APT group only targeted a small number of victims over short periods of time with each ransomware family. These short periods and small number of victims prevent too much attention being drawn from security researchers, leading to attribution to ransomware groups instead of an APT group. Such characteristics are not in line with how typical ransomware affiliates operate; affiliates usually conduct as many attacks as possible against multiple organizations to garner the most financial gains from their criminal activity. In this case, Bronze Starlight carefully selected targets with high-valued IP that is deemed valuable to the Chinese government, and did not attack other organizations that did not have seemingly valuable information or data. Bronze Starlight is also reported to have made use of the HUI Loader, along with a relatively rare version of PlugX, a remote access trojan (RAT) linked exclusively to China-backed threat groups.

HUI Loader filename	Payload filename	Cobalt Strike C2 domain	Ransomware
active_desktop_render.dll	desktop.ini	sc . microsofts . net	LockFile
Lockdown.dll	mfc.ini	update . ajaxrenew . com	AtomSilo
Lockdown.dll	sets5s.ini	Unknown (payload file unavailable for analysis)	Rook
Lockdown.dll	Lockdown.conf	api . sophosantivirus . ga sub . sophosantivirus . ga	Night Sky
libcef.dll	utils.dll	api . sophosantivirus . ga	Night Sky
LockDown.dll	vm.cfg	peek . openssl-digicert . xyz	Pandora

Figure 15: HUI Loader and Cobalt Strike Beacon samples linked to ransomware activity used by Bronze Starlight (Source: Secureworks)

Outlook

We believe that the semiconductor industry will remain an attractive target for ransomware gangs and other cybercriminals conducting cyberattacks. With more funding from the US government in the form of the CHIPS and Science Act to support the US domestic semiconductor industry, there is great potential for expansion and growth within the industry and we believe this trend will provide a much stronger incentive for financially motivated ransomware threat actors and affiliates to attack semiconductor firms belonging to the US and its allies, such as Taiwan, South Korea, and Japan. While we did not find direct links between the aforementioned cyberattacks on semiconductor companies and cyber espionage by state-sponsored threat actors, we believe that it is highly possible for financially motivated operators to leverage US-China and US-Russia tensions to sell IP-related materials to nation-states.

World-class domestic semiconductor design and manufacturing has long been a national strategic objective of China. This self-reliance is especially vital in times of war, when possible international sanctions could put a stop to semiconductor imports. The fierce competition for semiconductor supremacy is at the heart of the geopolitical struggle between China and Taiwan, as well as the entire Asia Pacific region; China's past advancement in semiconductors has already been linked to alleged espionage. We do not rule out the possibility of nation-state involvement in these ransomware attacks on semiconductor companies. Furthermore, nation-states could also hide behind the facade of ransomware operators and their affiliates, and are not likely to take responsibility for IP and data theft of semiconductor firms. Threat groups operating in the interests of nation-states, such as Bronze Starlight, have already utilized multiple strains of ransomware to encrypt, steal, or destroy IP data.

Despite a rise in US-China tensions over Speaker Pelosi's visit, we believe that a military conflict is not likely in the near future. However, instead of a direct military confrontation, there is a high likelihood of China conducting cyber warfare against Taiwan and the US, with semiconductor firms being a possible target. We believe that China, Russia, and North Korea have the intention, capabilities, and political will to conduct cyberattacks against the US and its allies, specifically top semiconductor firms such as TSMC and Samsung. We expect cybercriminals to conduct cyberattacks not just against these semiconductor firms directly, but also against their partner companies, clients, and raw material suppliers.

Any delays or disruptions to the semiconductor industry in the current semiconductor chip shortage situation will have a detrimental impact on the production capabilities of industries across the globe, and may result in worsening economic conditions around the world. This in turn may also lead to future social unrest and political shifts due to economic hardship, which will serve the political, military, economic, and technological interests of nation-states such as China and Russia.

Appendix A: Mitigations

In ransomware attacks, there is no guarantee that data will be released, decrypted, or secured after payment is made. However, to strengthen the security posture of an organization, we recommend the following mitigations to reduce overall ransomware risk and impact:

- Maintain offline backups of sensitive data and ensure these backups stay up-to-date to prevent data loss in the event of a ransomware infection.
- Network segmentation can halt the propagation of ransomware through an organization's network. This solution involves splitting the larger network into smaller network segments and can be accomplished through firewalls, virtual local area networks, and other separation techniques.
- Exposed remote desktop protocol (RDP) servers are also abused by threat actors to gain initial access into a target's network. Threat actors will look for networks that have internet-facing servers running RDP and then exploit vulnerabilities in those servers or use brute-force password attacks. Once inside the network, the threat actors can move laterally and install their ransomware on target machines, often disabling backups and other protections. If remote access solutions are crucial to daily operations, all remote access services and protocols, such as Citrix and RDP, should be implemented with multi-factor authentication (MFA).
- In addition to MFA, end users can reduce the risk of being victimized by a brute-force attack by using a password manager and setting a unique strong password for each online account.
- Through the use of process monitoring, monitor for the execution and command of binaries involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit.
- Monitor for the creation of suspicious file modification activity, particularly large quantities of file modifications in user directories.
- Consider keeping sensitive client information on systems that are disconnected from the internet or segmented from the rest of the corporate network. Since ransomware will encrypt all files on a victim system and often search for directories on the network (like networked file shares) to also encrypt, moving highly sensitive customer data to a system with no internet access or access to the rest of the network would help minimize ransomware's access to such data.
- Entities should also closely track the victims and third parties that are identified on extortion sites for potential links to their own organization, which can provide a convenient entry for threat actors looking to gain initial access. The highly sensitive information shared on the extortion sites can be used for phishing, spearphishing, spoofing, and other types of attacks, and organizations should heighten their security posture with any entity identified on these sites. We publish regular updates on victims and third parties identified on extortion sites.
- In the event of a successful ransomware deployment, it is recommended to not pay the ransom as it could run afoul of US Treasury Department OFAC/FINCEN rules, and only encourages threat actor behavior.

Ransomware often follows a specific pattern of behavior that can be detected with a robust threat intelligence system, integrated with SIEM platforms. In addition, organizations can implement YARA rules like the ones found in Recorded Future® Hunting Packages to identify malware via signature-based detection or SNORT rules for endpoint-based detections.

This report includes information gathered using the Recorded Future® Platform, dark web sources, and open-source intelligence techniques (OSINT).

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.